Nineteen Hundred and Twenty-two

NYIPLA®

New York
Intellectual Property
Law Association

SolarWinds – Pandora's Box of Cybersecurity and Data Risks

Robert C. Atkinson, M&T Bank
Kevin Jordan, McKinsey & Company
Diana Santos, Memorial Sloan Kettering Cancer Center
Adrienne Valencia Garcia, IBM
Moderator **Jessica Copeland**, Bond Schoeneck & King

What is SolarWinds?

- A major United States information technology firm.
- It is a networking software company that helps other companies manage their entire IT portfolios.
- Specifically, the Orion product that was breached provides centralized monitoring across an organization's entire IT stack.
  - This means the hackers were able to gain a very high level of access to SolarWinds Client's systems.
  - SolarWinds has 33,000 customers who use Orion.

What Happened?

- In March of 2020, SolarWinds sent out a software update to its Orion customers. Unbeknownst to SolarWinds, the software update had been compromised and contained hacked code.
- The code created a backdoor to customer's information technology systems.
- The hackers then used this backdoor to install even more malware into the systems.
    - This helped them spy on companies and organizations.

What Happened?

- This breach went unnoticed for months.
- In December of 2020 FireEye, a prominent cybersecurity firm, discovered they were a victim of an attack and were able to link the attack back to the SolarWinds backdoor.

How did this happen?

- Like most cyber intrusions, human error is often to blame.
- According to the Verizon Business Data Breach Investigation Report, in 2020 85% of breaches involved a human element.
- 36% of all attacks involved phishing, and more than 10% involved ransomware.
- A joint study from Stanford University Professor Jeff Hancock and security firm Tessian revealed that nine in 10 (88%) data breach incidents are caused by employees' mistakes.
  - One in four employees said that they have clicked on phishing emails at work.
  - The top reasons for clicking on phishing emails are the perceived legitimacy of the email (43%) and the fact that it appeared to have come from either a senior executive (41%) or a well-known brand (40%).

Major Companies and Agencies Were Compromised

- Of what is known currently, over 100 private sector companies and 9 federal agencies were compromised.
- **Agencies:** US Treasury, Commerce, State, Energy, Homeland Security, National Nuclear Security Administration.
- **Companies:** Intel, Nvidia, Cisco, Belkin, VMWare, Microsoft, FireEye, Deloitte, and other organizations like the California Department of State Hospitals, and Kent State University

Why is it a big deal?

- Because so many organizations and government agencies were compromised, it’s expensive and difficult to fix and secure.
- It could be years before networks are secure again.
    - With access to government networks, hackers could, "destroy or alter data, and impersonate legitimate people," Tom Bossert, President Trump's former homeland security officer, Op-Ed for the New York Times.
- Major Wake Up Call for the Federal Government: The US Cyber Command did not detect the attack before a private company did. Instead, a private company was the first to notice.

Biden Administration Response to Breach

- Executive Order titled "Improving the Nation's Cybersecurity."
  - Sets forth guidelines and a timeline for the development of new IT rules for federal agencies and contractors, implementation of additional IT security measures for agencies and contractors, enhanced software supply chain security, mandatory federal cyber incident reporting, standardized government response and a cybersecurity national review board.
- Sanctions against Russia
  - The White House issued a directive to expel ten diplomats and place other sanctions on Russian individuals and assets, including blacklisting 30 entities.

Prevention- Vendor Management Best Practices

- Policies: Info Security Plan, Risk Assessment, Data Restriction, Incident Response Plan.
- Identify and understand nature of data collected and used by business.
- Physical, administrative, and technical safeguards.
- Employee Training

Recent News

- May 24, 2021: According to **Microsoft**, the hackers behind the SolarWinds breach have launched another cyberattack.
- Microsoft refers to the group as "Nobelium."
- 3,000 email accounts of over 150 organizations were targeted
  - Targets included government agencies, think tanks, consultants, and non-governmental organizations.
  - Organizations in the United States received the largest share of attacks, but targeted victims span 24 countries.

Recent News - Colonial Pipeline

- **What Happened:** Ransomware attack that stole almost 100 gigabytes of data and shut down one of America's most important pieces of infrastructure.
  - Largest pipeline system for refined oil product in the U.S. (5,500 miles long).
  - Although not carried out by the same group as SolarWinds, this cyber-criminal organization was also connected to Russia.
- **Effects:** Thousands of gas stations without fuel, increased gasoline prices, and panic across the East Coast.
- **Enhanced Regulations:** Cybersecurity regulations are now mandatory for leading pipeline companies in the U.S.: (1) required to report all cyberattacks to the federal authorities; (2) designate a "Cybersecurity Coordinator" who is available 24/7; (3) create a timeline for remedying possible flaws; and (4) complete an assessment of current practices compared to government regulations.
  - Companies that do not comply with the regulations will be sanctioned daily.

Recent News – JBS Foods

- **What Happened:** Cyberattack that resulted in suspended operations in JBS processing plants across North America and Australia.
  - JBS Foods is one of the largest food companies in the world.
  - Believed that the cyber-criminal organization did not access or compromise any employee, supplier, or customer data.
- **Effects:** JBS was unable to process thousands of carcasses, which delayed transactions with suppliers and customers.
- **Government Response:** The U.S. government has taken an active stance in directly dealing with the Russian government and has assisted in mitigating the impact of the attack on the nation’s meat supply.
  - Although not carried out by the same group as SolarWinds, this cyber-criminal organization was also connected to Russia.

Strategy & Practical Guidance

- Leverage in negotiations, find your opening but recognize where you stand in the relationship
- Vendor/asset management system
- Reasoning behind regulation and why organization can push for more indemnification
  - Time to properly preview SW updates
- Wholistic approach to vendor engagement
  - Allocate resources to assess technical risks and address necessary remediations
  - Allocate resources to stay up to date with technical risks and implement policies, educate business teams, etc.